CONDITIONAL ACCESS SYSTEM FOR DIGITAL RECEIVERS

Field of the Invention

This invention concerns a system for providing conditional access (i.e., managing access) to a received scrambled audio/visual (A/V) signal from a variety of sources, such as, broadcast television networks, cable television networks, digital satellite systems, and internet service providers. Utilizing the concept of secret sharing, the system does not require full descrambling keys to be sent to the receiving device under encryption. The keys are recovered using a seed value received from the service provider and a seed value stored in the device.

Background of the Invention

Today, a user may receive services from a variety of service providers, such as broadcast television networks, cable television networks, digital satellite systems, and internet service providers. Most television receivers are capable of receiving unscrambled information or programs directly from broadcast and cable networks. Cable networks providing scrambled (or encrypted) programs usually require a separate stand alone set-top box to descramble (or decrypt) the program. Similarly, digital satellite systems usually provide scrambled programs that also require the use of a separate set-top box. These set-top boxes may utilize a removable smart card which contain the keys necessary for recovering the scrambling or descrambling keys. Protection of these important keys is paramount to prevent unauthorized copying of the programming.

European Patent Application Number EP-A-0 658 054 discloses generating a descrambling key using two pieces of transmitted data.

Summary of the Invention

In a conditional access (CA) system, the signals are usually scrambled using symmetric ciphers such as the Data Encryption Standard (DES). For security reasons, the scrambling key is

changed frequently, the period of change being as frequent as every few seconds. The protection of the descrambling keys, which need to be sent with the signals, is often provided by public-key cryptography. Public-key cryptography introduces problems associated with the public key infrastructure and distribution of the keys. This invention resides, in part, in recognition of the described problem and, in part, in providing a solution to the problem.

A signal (e.g., an event or program) as described herein comprises information such as (1) audio/visual data (for example, a movie, weekly "television" show or a documentary); (2) textual data (for example, an electronic magazine, paper, or weather news); (3) computer software; (4) binary data (for example, images); (5) HTML data (for example, web pages); or any other information for which access control may be involved. The service providers include any provider broadcasting events, for example, traditional broadcast television networks, cable networks, digital satellite networks, providers of electronic list of events, such as electronic program guide providers, and in certain cases internet service providers.

Generally, the present invention defines a method for managing access to a signal, representative of an event of a service provider, utilizing a smart card. That is, this method comprises receiving in a smart card, a signal that is scrambled using a scrambling key, receiving data representative of a first seed value, generating the scrambling key using the first seed value and a second seed value that is stored in the smart card and descrambling the signal using the generated scrambling key to provide a descrambled signal.

In accordance with one aspect of the present invention, the first and second seed values are points on a Euclidean plane and the step of generating the scrambling key comprises calculating

the Y-intercept of the line formed on the Euclidean plane by the first and second seed values.

In accordance with still another aspect of the present invention, a system for managing access between a service provider and a device having a smart card coupled to the device involves the device performing the steps of receiving from the service provider a signal representative of an event that is scrambled using a scrambling key, receiving from the service provider data representative of a first seed value selected from a Euclidean plane, and coupling the scrambled signal and the first seed value to the smart card. The smart card has a means for access control processing comprising means for generating a scrambling key by calculating the Y-intercept of the line formed in the Euclidean plane by the first seed value and a second seed value stored in the smart card and means for descrambling the signal using the generated scrambling key to generate a descrambled signal.

These and other aspects of the invention will be explained with reference to a preferred embodiment of the invention shown in the accompanying Drawings.

Brief Description of the Drawing

Figure 1 is a block diagram illustrating one architecture for interfacing a common set-top box to a variety of service providers.

Figure 2 is a block diagram of an exemplary implementation of a system for managing access to a device in accordance with the invention;

Figure 3a is a graphical representation of the determination of the scrambling key in accordance with one embodiment of this invention; and

Figure 3b is a graphical representation of an allocation of a unique and non-overlapping range for each service provider in accordance with Figure 3a.

Detailed Description of the Drawing

The present invention provides a conditional access system which may be utilized to obtain services from one of a plurality of sources. The conditional access system when implemented within a device, such as a digital television, digital video cassette recorder or set-top box, provides convenient management of the descrambling keys because only a portion of the seed value necessary for key generation is stored therein. For simplicity, the below description of the invention will be directed towards an implementation using a digital television and a smart card.

In Figure 1, system 30 depicts the general architecture for managing access to a digital television (DTV) 40. Smart Card (SC) 42 is inserted into, or coupled to, a smart card reader 43 of DTV 40; an internal bus 45 interconnects DTV 40 and SC 42 thereby permitting the transfer of data therebetween. Such smart cards include ISO 7816 cards having a card body with a plurality of terminals arranged on a surface in compliance with National Renewable Security Standard (NRSS) Part A or PCMCIA cards complying with NRSS Part B. Conceptually, when such a smart card is coupled to a smart card reader, the functionality of the smart card may be considered to be a part of the functionality of the device (e.g., DTV 40) thus removing the "boundaries" created by the physical card body of the smart card.

DTV 40 can receive services from a plurality of service providers (SPs), such as a broadcast television SP 50, a cable television SP 52, a satellite system SP 54, and an internet SP 56. Conditional Access Organization (CA) 75 is not directly connected to either the service providers or STB 40 but deals with key

management and issues public and private key pairs which may be used, if necessary, as explained below.

The present invention employs the concept of secret sharing which eliminates the requirement for using public key cryptography to ensure secure transmission of the audio/visual (A/V) stream from a service provider. A variation of a secret sharing scheme, developed by Adi Shamir, is known as a threshold scheme. An (m, n) threshold scheme involves breaking a secret into n pieces (which may be called shadows), in such a way that at least m (<=n) of the pieces are required to reconstruct the secret. A perfect threshold scheme is a threshold scheme in which a knowledge of m-1 or fewer shadows provides no information about the secret. For example, with a (3,4)-threshold scheme, the secret is divided into four portions but only three of the four portions are required to reconstruct the secret. Two of the portions, however, cannot reconstruct the secret. In Shamir's (m, m) threshold scheme, choosing a higher value for m, and storing (m-1) secrets in the card would increase the system's resistance to ciphertext only attacks, but would lead to more computations for polynomial construction.

Such a threshold scheme reduces the computational requirements for the card in DES key recovery. For each new key, only a simple operation is performed (i.e., the value of the polynomial at x = 0 is computed) as compared to RSA decryption which involves modular exponentiation. Additionally, security is "perfect" (i.e., given knowledge of (x_1, y_1), all values of the secret remain equally probable).

Figures 2 and 3 together, demonstrate one embodiment of the present invention. Particularly, stored in SC 42 is a first seed value (or data point). The first seed value may be thought of as a single point on a Euclidean plane, i.e., in the form of (x0, y0). Service provider 58 transmits a signal (or event or program) that may be scrambled by a symmetric key, for example a Data Encryption Standard (DES) key. In addition to the scrambled

signal, service provider 58 transmits a second seed value. Similarly, the second seed value may be a second single point from the same Euclidean plane, i.e., in the form of (x1, y1).

The scrambled A/V signal and the second seed value is received by DTV 40 and is coupled to SC 42 for processing. SC 42 receives the second seed value and utilizes both the stored first seed value and the received second seed value to reconstruct (or recover) the symmetric key. SC 42 uses the reconstructed symmetric key to descramble the received scrambled A/V signal and generate a descrambled A/V signal. This descrambled A/V signal is provided to DTV 40 for display.

Recovery of the symmetric key is achieved by constructing a polynomial utilizing the first and the second seed values; the y-intercept of the constructed polynomial is the symmetric key. For example, given (x0, y0) and (x1, y1), the symmetric key is constructed by computing the value of $[\{(y1-y0)/(x1-x0)\}(x-x0)] + y0$ at $x = 0$. Figure 3a illustrates a graphical representation of the present invention.

Such an approach permits more than one service provider to share the stored second seed value (x0, y0). Each service provider would then be free to choose its own first seed value. The probability of constructing polynomials with identical y-intercepts (i.e., identical symmetric keys) is low. However, the range of possible second seed values could be allocated such that each service provider has a unique and non-overlapping range (see Figure 3b). Further, it is within the scope of the present invention that each service provider could choose its own first seed value which could be encrypted using the public key of the smart card before downloading. The seed value would be recovered by the smart card using its stored private key (K_{SCpri}).

The general architecture of system 30 lends itself to achieving the goal of minimizing the amount of information (or

keys) that needs to be stored in a smart card to permit access to more than one service provider.

The robustness of the defined system may be increased by scrambling portions of the event with different keys and transmitting different second seed values. Further, it is within the scope of the present invention that more than two seed values may be used to recover the symmetric key. For example, two or more seed value may be stored in the smart card and a seed value may be transmitted with the encrypted A/V signal. The symmetric key would be recovered using all of the seed values.

While the invention has been described in detail with respect to numerous embodiments thereof, it will be apparent that upon reading and understanding of the foregoing, numerous alterations to the described embodiment will occur to those skilled in the art and it is intended to include such alterations within the scope of the appended claims.